IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

EDWIN CABRERA, KEVIN CAMORLINGA, AUSTIN RICHARD, ANDREW SKALAK, and MARK SULLIVAN, on behalf of themselves and all other similarly situated individuals, Plaintiffs, v. LEDGER SAS and LEDGER TECHNOLOGIES, INC., Defendants.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Edwin Cabrera, Kevin Camorlinga, Austin Richard, Andrew Skalak, and Mark Sullivan (collectively, "Plaintiffs") bring this putative class action against Defendants Ledger SAS ("Ledger") and Ledger Technologies, Inc. ("Ledger Technologies") (collectively, "Defendants"). Plaintiffs' allegations regarding their own experiences are based on their personal knowledge. Plaintiffs' allegations regarding all other matters are based on information and belief, informed by counsel's reasonable investigation.

I. INTRODUCTION

1. This action arises out of false and misleading statements that Ledger made about the cryptocurrency hardware wallets it produces. Hardware wallets, including the Ledger Nano S and Ledger Nano X ("Nano Wallets"), are devices that hold alphanumeric codes known as "private keys." A private key is like a password to a cryptocurrency bank account; anyone who learns a private key can transfer the cryptocurrencies it protects. The same is true for "seed phrases," which are phrases from which private keys can be mathematically derived.

2. Private keys are frequent targets for bad actors. Criminals have stolen billions of dollars in cryptocurrency online using hacking and malware. They have also stolen crypto-assets using "social engineering" attacks, in which they acquire private keys from employees of companies that store them for customers.

3. Ledger marketed Nano Wallets as a solution to these threats. Nano Wallets, ostensibly, permit users to independently create and store private keys offline using a "Secure Element" chip within the wallets' hardware. Ledger said these keys "always" remain offline and can "never leave the security of the hardware, even when connecting your wallet to your smartphone or desktop."[1] It said even a "firmware update cannot extract the private keys" from Nano Wallets, meaning Ledger itself could never access them.[2]

4. These claims were false. In May 2023, Ledger announced a new Nano Wallet feature called "Ledger Recover" or simply "Recover." Recover backs up customers' private keys by extracting seed phrases from Nano Wallets, over the internet, via a firmware update. As news of the Recover feature spread, Ledger admitted: "Technically speaking it is and *always has been* possible to write firmware that facilitates key extraction. You have always trusted Ledger not to deploy such firmware whether you knew it or not."

5. This provoked outrage among Ledger's customers and the cryptocurrency community at large. In particular, Ledger's social media pages suffered an onslaught of negative comments from infuriated users. One complained: "I bought ledgers (multiple) as I was led to believe it was impossible for the secure chip to leak the key, intentional or not. But here is Ledger

[1] Nano Wallet users must connect their wallets to smartphones, computers, or other devices to complete transactions in the cryptocurrencies protected by those wallets.

[2] Firmware is a type of software that is specific to, and embedded in, a physical device and is intended to help the device function.

just adding the very functionality that I thought the chip was designed to prevent. I've been scammed." Another said: "The premise the seed stayed secure on the chip was [Ledger's] entire business model which we now know was a lie all along." Another person stated: "NOBODY NOT A SINGLE PERSON ASKED FOR THIS. Totally annihilates the entire purpose of owning a Ledger." And as another person succinctly put it: "Liars gonna lie. Bye Ledger."

6. Ledger users did not just vent their frustration online. They changed their behavior. Many stopped using Ledger wallets to secure their cryptocurrency, viewing the devices as functionally worthless based on the Recover revelations.[3] Tellingly, in the weeks following those revelations, Trezor—another hardware wallet producer—experienced a 900% increase in sales as customers abandoned Ledger.

7. Plaintiffs in this case are among the cryptocurrency users that Ledger hoodwinked. They each purchased Nano Wallets at prices artificially inflated by Ledger's inaccurate statements about the wallets' security features. Had they known those statements were inaccurate or misleading, they would not have purchased the devices at all.

8. Actions have consequences. The law does not permit companies to enrich themselves, at consumers' expense, through misrepresentations and omissions about their products. Plaintiffs and similarly situated Ledger customers are entitled to damages based on Ledger's history of deceptive practices surrounding its Nano Wallets.

II. PARTIES

9. Plaintiff Edwin Cabrera is an Illinois resident. While in Illinois in 2022, he conducted research into cryptocurrency hardware wallets because he was concerned that his cryptocurrency would not be safe with a custodial service. He read about Ledger wallets on

[3] Herein, the phrases "Nano Wallet" and "Ledger wallet" are used interchangeably.

Ledger's website. He does not recall the information he read word-for-word, but he recalls that Ledger claimed (a) it is not possible for private keys to leave Ledger wallets or be exposed to the internet; (b) no one aside from a Ledger wallet's owner can access private keys stored on a Ledger wallet; and (c) Ledger wallets provide users with complete ownership and control over their private keys and, by extension, the cryptocurrencies they protect. Relying on those and similar representations, while in Illinois, Mr. Cabrera purchased a Ledger Nano S Plus[4] and a Ledger Nano X in July 2022 by ordering it off of Ledger's website to be delivered to Mr. Cabrera in Illinois. Had Mr. Cabrera known the representations he read on Ledger's website were false or misleading, he would not have purchased either of the Ledger wallets. Mr. Cabrera has not updated the firmware for his Ledger Nano X since Ledger announced the Recover feature in May 2023 because he does not want to risk using firmware with key-extraction capabilities. He understands that without firmware updates, his Ledger Nano X will become unusable.

10. Plaintiff Kevin Camorlinga is an Illinois resident. While in Illinois in 2021, he read about Ledger wallets on Ledger's website. He does not recall the information he read word-for-word, but he recalls that Ledger claimed (a) it is not possible for private keys to leave Ledger wallets or be exposed to the internet; (b) no one aside from a Ledger wallet's owner can access private keys stored on a Ledger wallet; and (c) Ledger wallets provide users with complete ownership and control over their private keys and, by extension, the cryptocurrencies they protect. Relying on those and similar representations, while in Illinois, Mr. Camorlinga purchased a Ledger Nano S in September 2021 by ordering it off of Ledger's website to be delivered to Mr. Camorlinga in Illinois. Had Mr. Camorlinga known the representations he read on Ledger's website were false

[4] A Ledger Nano S Plus is a Ledger Nano S with a larger screen and more storage capacity. Outside of Part II of this Complaint, "Ledger Nano S" refers to both versions of the Ledger Nano S. Throughout this Complaint, the phrases "Nano Wallet" and "Ledger wallet" include both versions of the Ledger Nano S.

or misleading, he would not have purchased the Ledger Nano S.

11. Plaintiff Austin Richard is an Illinois resident. While in Illinois in 2020, he read about Ledger wallets on Ledger's website. He does not recall the information he read word-for-word. But he recalls that Ledger claimed (a) it is not possible for private keys to leave Ledger wallets or be exposed to the internet; (b) no one aside from a Ledger wallet's owner can access private keys stored on a Ledger wallet; and (c) Ledger wallets provide users with complete ownership and control over their private keys and, by extension, the cryptocurrencies they protect. Relying on those and similar representations, while in Illinois, Mr. Richard purchased a Ledger Nano S and a Ledger Nano X in approximately July 2020 by ordering it off of Ledger's website to be delivered to Mr. Richard in Illinois. Had Mr. Richard known the representations he read on Ledger's website were false or misleading, he would not have purchased either of the Ledger wallets. Mr. Richard has not updated the firmware for his Ledger Nano X since Ledger announced the Recover feature in May 2023 because he does not want to risk using firmware with key-extraction capabilities. He understands that without firmware updates, his Ledger Nano X will become unusable.

12. Plaintiff Andrew Skalak is an Illinois resident. While in Illinois in 2018, he read about the Ledger Nano S on Ledger's website. He does not recall the information he read word-for-word. But he recalls that Ledger claimed (a) it is not possible for private keys to leave Ledger wallets or be exposed to the internet; (b) no one aside from a Ledger wallet's owner can access private keys stored on a Ledger wallet; and (c) Ledger wallets provide users with complete ownership and control over their private keys and, by extension, the cryptocurrencies they protect. Relying on those and similar representations, while in Illinois, Mr. Skalak purchased a Ledger

Nano S in January 2018 by ordering it off of Amazon to be delivered to Mr. Skalak in Illinois.[5] Had Mr. Skalak known the representations he read on Ledger's website were false or misleading, he would not have purchased the Ledger Nano S.

13. Plaintiff Mark Sullivan is an Illinois resident. While in Illinois in April 2023, he purchased a Ledger Nano X by ordering it off of Ledger's website to be delivered to him in Illinois. Before purchasing his Ledger Nano X, while in Illinois in 2023, Mr. Sullivan read information on Ledger's website. He does not recall the information he read word-for-word. But he recalls that Ledger claimed that (a) it is not possible for private keys to leave Ledger wallets or be exposed to the internet; (b) no one aside from a Ledger wallet's owner can access private keys stored on a Ledger wallet; and (c) Ledger wallets provide users with complete ownership and control over their private keys and, by extension, the cryptocurrencies they protect. Mr. Sullivan relied on those and similar representations in purchasing his Ledger Nano X. Had Mr. Sullivan known the representations he read on Ledger's website were false or misleading, he would not have purchased the Ledger Nano X. Mr. Sullivan has not updated the firmware for his Ledger Nano X since Ledger announced the Recover feature in May 2023 because he does not want to risk using firmware with key-extraction capabilities. He understands that without firmware updates, his Ledger Nano X will become unusable.

14. Defendant Ledger is a simplified joint-stock company headquartered at 1 Rue du Mail, 75002 Paris, France.

15. Defendant Ledger Technologies is a Ledger subsidiary incorporated in Delaware. Its principal place of business is 368 9th Avenue, 6th Floor, New York, NY 10001. It is registered

[5] Ledger wallet purchases made on Amazon are made "directly from Ledger," as Amazon is an authorized distributor of Ledger products. https://support.ledger.com/hc/en-us/articles/4404389367057-Is-my-Ledger-device-genuine-?docs=true (last visited January 7, 2024).

to do business in New York as a Foreign Business Corporation.

III. JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this matter under 28 U.S.C. § 1332(a) because the amount in controversy exceeds $75,000 exclusive of interest and costs and there is diversity of citizenship between the parties.

17. This Court also has subject matter jurisdiction over this matter under 28 U.S.C. § 1332(d) because this is a class action with more than 100 class members, there is diversity of citizenship among the parties, and the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

18. This Court also has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1367 because this matter asserts federal and state-law causes of action that form part of the same case or controversy.

19. This Court has specific personal jurisdiction over Ledger because Ledger has purposefully directed its activities at Illinois and/or purposefully availed itself of the privilege of conducting business in Illinois, and Plaintiffs' injuries arise out of Ledger's Illinois-related activities.

20. Ledger set up an interactive website for the sale of its products and explicitly provided that Illinois residents can purchase those products from its website. The website requires customers to select a shipping address, and Illinois is one of the "ship-to" options available on Ledger's drop-down menu.

21. After an Illinois resident creates a purchase order on Ledger's website (whether for a Nano Wallet or a different product), Ledger sends them an email thanking them for their order, confirming their order number, and listing their Illinois shipping address.

22. In the same email, Ledger includes advertisements and promotional statements,

such as: "Ledger. The gateway to buy, store, exchange, sell, and grow your assets with our partners. Easily and securely." Ledger also encourages the Illinois resident to use Ledger's services, such as by downloading the "Ledger Live" application.

23. Next, Ledger ships its products to the Illinois resident and sends them a second email. The second email confirms the resident's products are on the way and again lists the resident's shipping address. The second email also contains advertisements for Ledger, such as the following:

- "Who are we? Ledger is the safe gateway to all your crypto needs. Ledger hardware wallets, together with our Ledger Live app, allow you to buy, sell, manage, exchange and grow your crypto. Securely & easily."
- "Unlock a world of crypto possibilities. Ledger hardware wallets combined with Ledger Live app give you access to an entire ecosystem of smart crypto services and dApps, from NFTs to DeFi – 100% securely, all in one powerful app."

24. Further, the second email encourages the Illinois resident to download Ledger Live, "explore our products," and "explore our catalogue," and it includes corresponding website links.

25. Once the Illinois resident's products arrive, Ledger sends them a third email informing them of the arrival and containing additional promotional statements. All three emails list "Ledger SAS, 1 rue du Mail, 75002 Paris" at the bottom of the email.

26. Within the package sent to the Illinois resident (e.g., within the package for a Nano Wallet), Ledger includes additional promotional materials. They include a card advertising the Ledger Live service, which states: "Start your crypto journey securely with Ledger Live." They also include a packet with stickers containing Ledger's name and logo, which Ledger hopes Illinois residents will affix to items like their laptops to assist in Ledger's marketing efforts in Illinois.

27. Ledger has purposefully sold tens of thousands of Nano Wallets to Illinois residents between June 20, 2016 and the present via the foregoing process, or a substantially similar process, including to Plaintiffs, and Plaintiffs' claims arise out of those sales.

28. This Court has specific personal jurisdiction over Ledger Technologies for the same reasons it has such jurisdiction over Ledger. Ledger Technologies is functionally the U.S. department of Ledger. Ledger Technologies is a wholly owned subsidiary of Ledger. Ledger Technologies is financially dependent on Ledger because Ledger Technologies has no source of income or operating capital separate from Ledger. Ledger Technologies does not operate its own website, sell its own products, or engage in any business activity disconnected from Ledger. Ledger and Ledger Technologies have overlapping officers and employees, and Ledger controls Ledger Technologies' affairs and operations. Both entities have the same Chief Executive Officer (Pascal Gauthier). Both entities also share offices, including in France and New York. Ledger simply uses Ledger Technologies to carry out U.S.-based activities.

29. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to this lawsuit occurred in this judicial district. Alternatively, venue is proper under 28 U.S.C. § 1391(b)(3) because Ledger and Ledger Technologies are subject to the Court's personal jurisdiction with respect to this lawsuit.

IV. FACTUAL ALLEGATIONS

A. Private keys and seed phrases control access to cryptocurrencies.

30. Cryptocurrencies are digital forms of money. Bitcoin is the first, and largest, cryptocurrency. It launched in the wake of the 2008 Global Financial Crisis as public trust in centralized banking institutions plummeted. Bitcoin permits users to store value, and transact with one another, online without relying on any third-party services. As some have put it, Bitcoin and other cryptocurrencies allow you to "be your own bank." Cryptocurrencies have historically appealed to consumers who highly value financial privacy and autonomy.

31. Although cryptocurrencies have traditionally occupied a niche market, they are becoming increasingly "mainstream." Thousands of crypto-assets have emerged in the years since

Bitcoin launched, the market capitalization of cryptocurrencies now exceeds $1.5 trillion, and approximately one in four Americans currently own cryptocurrency.

32. Understanding how cryptocurrency works requires an understanding of private keys and seed phrases. A private key is a long string of letters and numbers that gives its owner control over cryptocurrency associated with the key. Seed phrases are collections of words from which private keys can be mathematically derived. In fact, a single seed phrase can be used to derive multiple private keys associated with a cryptocurrency wallet; it is like a "master key for your private keys." https://www.ledger.com/academy/basic-basics/2-how-to-own-crypto/whats-a-secret-recovery-phrase (last visited January 4, 2024). Anyone who learns a private key or a seed phrase can steal all of the cryptocurrency associated with it.

33. For that reason, an oft-repeated phrase within the cryptocurrency community is "not your keys, not your coins." In other words: if you permit others to store or access your private keys, you do not truly own any of the cryptocurrencies they control.

B. Cryptocurrency users buy hardware wallets because they offer security features including self-custody, exclusive ownership, and offline storage of private keys.

34. Cryptocurrency users have several options for storing their private keys. For one, they may entrust their keys to cryptocurrency exchanges or other custodial service-providers. But these third parties have not reliably kept customers' private keys safe. Many have lost customer funds to online hackers. *E.g.*, Evelyn Cheng, *Japanese Cryptocurrency Exchange Loses More Than $500 Million to Hackers*, CNBC (January 26, 2018), https://tinyurl.com/37tmse4v. Others have lost customer funds to social engineering attacks. *E.g.*, *Social Engineering Enabled $37 Million Theft From Crypto Firm*, PMNTS (August 7, 2023), https://tinyurl.com/mu62pmw5. And in some cases, employees of an exchange or custodian itself have drawn customer funds directly

from customers' wallets and used them for personal gain. *E.g.*, Marley Jay & Phil Helsel, *Sam Bankman-Fried Found Guilty on all Counts at Fraud Trial Over Crypto Exchange FTX*, NBC NEWS (November 2, 2023), https://tinyurl.com/wr8eb4us.

35. Some cryptocurrency users, wary of entrusting their keys to third parties, use an alternative option: software wallets. Software wallets allow users to "self-custody" their private keys. That is, a user can download a software application to a smartphone or other device, and then they can independently create and store private keys without entrusting the keys to another entity. *See What is a Software Wallet?*, LEDGER (October 26, 2023), https://tinyurl.com/yc8dknst.

36. There is a catch though. Software wallets expose private keys to the internet. *Id.* So, they are susceptible to hackers and malware. *Id.* Many cryptocurrency users have lost funds by relying on software wallets. *E.g.*, Carly Page, *North Korean Hackers Linked to Atomic Wallet Crypto Hack*, TECHCRUNCH (June 8, 2023), https://tinyurl.com/3mbpcfak.

37. That is where hardware wallets come in. Hardware wallets permit users to independently create private keys, and self-custody those keys, just like software wallets. *See What Is a Hardware Wallet?*, LEDGER (October 26, 2023), https://tinyurl.com/2fbuyacp. And, like software wallets, hardware wallets do not expose users to the risk that employees of an exchange or custody service will steal or lose their private keys. But hardware wallets have an advantage over software wallets: they can store private keys, and facilitate transactions with them, without exposing them to the internet.[6] Many believe hardware wallets, when functioning as advertised, offer the "best of all worlds" for storing private keys.

38. Accordingly, cryptocurrency users pay a premium to store their private keys on

[6] Private keys are used to "sign" transactions in cryptocurrencies, which is required to complete the transactions. By permitting users to sign transactions offline, within the hardware wallet itself, hardware wallets are meant to reduce risks associated with online key exposure while still permitting wallet owners to transact in their cryptocurrency.

hardware wallets. Software wallets may be downloaded and used for free. *E.g.*, *Download Trust Wallet*, https://trustwallet.com/download (last visited January 1, 2024). Similarly, most cryptocurrency exchanges permit users to store funds thereon without charge. *E.g.*, *Create a Coinbase Account*, COINBASE (last visited January 1, 2024), https://tinyurl.com/mtxz3ekd ("Coinbase doesn't charge a fee to create or maintain your Coinbase account."). Yet customers will pay substantial sums for hardware wallets.

C. Ledger designs, manufactures, and sells cryptocurrency hardware wallets.

39. Ledger sells cryptocurrency hardware wallets. The company was founded in 2014 and was, at the time, one of the few hardware wallet companies in the world. Ledger sold its first Ledger Nano S on June 20, 2016. It sold its first Ledger Nano X on May 15, 2019.

40. The Ledger Nano S and the Ledger Nano X are identical in all relevant respects. *See Compare Ledger Hardware Wallets*, LEDGER (product comparison page from Ledger's website archived from May 18, 2022), http://tinyurl.com/2drwkza4. They each are rectangular devices with two buttons, a USB connector, and an electronic screen used to scroll through options and enter commands. They each include two computer chips. One, the Secure Element chip, stores private keys. The other, a microcontroller unit or "MCU" chip, helps link the Secure Element to outside interfaces, such as laptops and smartphones, so that users can execute cryptocurrency transactions using their Nano Wallets.

41. The primary difference between the Ledger Nano S and the Ledger Nano X is that the latter is meant for "one-the-go" use and is Bluetooth compatible. The current price of a Ledger Nano S is $79 and the current price of a Ledger Nano X is $149.

42. Ledger designs the hardware for its Nano Wallets. It has a dedicated hardware development team specifically for that purpose. Kirsty Moreland, *The Ledger Donjon*, LEDGER

(October 23, 2019), http://tinyurl.com/4y25w7tt. It also manufactures the hardware in-house. As Ledger has put it: "All parts are custom built by ourselves and we have our own assembly lines located in the center of France." *Ledger FAQ*, LEDGER (June 14, 2017), http://tinyurl.com/ycvyf3nd. Ledger products are also packaged in France.

43. Ledger also writes and updates the firmware and software for its Nano Wallets, via its firmware development team. Kirsty Moreland, *The Ledger Donjon*, LEDGER (October 23, 2019), http://tinyurl.com/4y25w7tt. Ledger's firmware team created the custom operating system used by Nano Wallets, the Blockchain Open Ledger Operating System also known as "BOLOS." *Introducing Bolos*, LEDGER (March 2, 2016), http://tinyurl.com/274wubfc.

44. Ledger is, and always has been, intimately familiar with the capabilities of its hardware wallets. Beyond the familiarity gleaned from inventing those wallets and writing their firmware, Ledger constantly reassesses its wallets' capabilities and vulnerabilities. It employs a team of "white hat hackers" in an "internal security evaluation lab" whose sole purpose is to "analyze and improve the security of Ledger products." Kirsty Moreland, *The Ledger Donjon*, LEDGER (October 23, 2019), http://tinyurl.com/4y25w7tt. The team works closely with Ledger's hardware and firmware teams to "continuously" evaluate Nano Wallets. *Id.*

D. Ledger told consumers its hardware wallets provide pure self-custody, exclusive ownership, and offline storage of private keys.

45. Ledger, cognizant of consumers' security preferences, and in an effort to induce consumers to purchase Nano Wallets, marketed Nano Wallets as offering pure self-custody, exclusive ownership, and offline storage of private keys through a long-term advertising campaign that originated in early 2016 and persisted through the present.

46. The campaign included video advertisements, online advertisements, statements from Ledger officers and employees, social media posts, product demonstrations at crypto-related

conferences, physical advertisements, statements on the packaging for Nano Wallets, and statements on Ledger's website, from which Ledger sells Nano Wallets.

47. Some of Ledger's video-advertisements featured famous Hollywood actors and cultural icons, such as Gwyneth Paltrow, Terry Crews, and Lizzie Armanto.

48. In 2019, Ledger even started "Ledger Academy," an informational program that ostensibly provides consumers with what they "need to learn about crypto safely." *Web3 Starts Here*, LEDGER (last visited January 1, 2024), http://tinyurl.com/2yvtm3sh. Through the "academy," Ledger has periodically published, on its website, articles and videos regarding cryptocurrency and Ledger's products. To date, Ledger has published nearly five hundred articles and videos via Ledger Academy.

49. Throughout Ledger's advertising campaign, Ledger repeated the same messages again and again, claiming: (a) it is not possible for private keys to leave Ledger wallets or be exposed to the internet; (b) no one aside from a Ledger wallet's owner can access private keys stored on a Ledger wallet; and (c) Ledger wallets provide users with complete ownership and control over their private keys. Examples of such statements include the following:

- "Your private keys are never held or known by Ledger or a third party: they are hard locked in the Secure Element. With Ledger Nano S, your wallet remains decentralized, you are your own bank." http://tinyurl.com/4xhn85vv (statement on Ledger's website from January 29, 2017).

- "[I]t is very important to understand that ***hardware wallet users control entirely their private keys***." http://tinyurl.com/4rfv3wf6 (statement on Ledger's website originally published on March 20, 2017) (emphasis added).

- "Can Ledger have access to my bitcoins? Absolutely not. Ledger will never have any knowledge of your master seed, private or public." http://tinyurl.com/ycvyf3nd (statement on Ledger FAQ page from June 3, 2017).

- "Ledger does not know your private keys. Ledger utilizes a decentralized wallet system. You generate the private keys on your Ledger device during the initialization process, and they are then stored within the Secure chip of your Ledger device. ***Ledger never has the opportunity to make a copy of your private***

keys." http://tinyurl.com/5n6ckeee (statement on Ledger FAQ page from March 23, 2018) (emphasis added).

- "No one can access your secrets. ***Your private keys are held in a Secure chip, and they never leave it***. Whenever a transaction is signed within the Secure chip, the private keys never become visible to the computer the Ledger device is connected to. A compromised computer will never be able to access the contents of the Secure chip." http://tinyurl.com/5n6ckeee (statement on Ledger FAQ page from March 23, 2018) (emphasis added).

- "Hardware wallets have been ***designed to make it impossible to access the private keys they protect, because they never leave the device***. This is called the principle of isolation, also known as cold storage. The private keys are never 'hot', or online, meaning they can never be exposed to the internet nor to the computer to which it's connected." http://tinyurl.com/2zssvdmf (statement on Ledger's website originally published on October 10, 2018) (emphasis added).

- "The secret keys or seed [on a Ledger wallet] . . . ***never, ever leave the Secure Element***." http://tinyurl.com/mry3hpvx (statement on Ledger's website originally published on January 15, 2019) (emphasis added).

- "Hardware wallets – such as a Ledger – are widely considered to offer the most secure wallet option for securing your crypto. . . . A hardware wallet ***stores your private keys offline, meaning nobody can access them except you***." http://tinyurl.com/3ktr4545 (statement on Ledger's website originally published on December 11, 2019) (emphasis added).

- "When you own crypto, what you really own is a private key that gives you access to your coins. You should be the only one in control of this key – and you need to keep it secure. . . . Your hardware wallet keeps your private key protected at all times in a certified secure chip. ***Nobody can access it except you***. . . . Your wallet also gives you the freedom to manage your crypto on your own. With the Ledger Live app, you can buy, exchange and grow your crypto securely – in one app. The brilliant association of those two elements brings you the satisfaction of real ownership – in simple words, ***the Ledger ecosystem enables you to be the only one in charge of your money***." http://tinyurl.com/5n8zx7ax (statement on Ledger's website originally published on December 11, 2019) (emphasis added).

- "[M]ore than ever, your private keys need to be offline under *your* control, nobody else's. . . . ***with Ledger, you can enjoy complete control*** over your assets, and complete peace of mind to go with it." http://tinyurl.com/muvff885 (statement on Ledger's website originally published on August 14, 2020) (emphasis added).

- "Ledger devices provide peace of mind to our users by offering an easy-to-use, accessible yet secure solution. In short: with our devices, you still own your keys, thus you securely own your own coins." http://tinyurl.com/2z5vshnr (statement on Ledger's website originally published on September 4, 2020).

- "[Nano Wallets are] the best way to secure your funds while giving you the freedom to manage everything *on your own*. This is how it works: your private key always remains offline in the hardware wallet. ***Nobody can access it or use it except you***." www.youtube.com/watch?v=aFQ1Z_Omz9U (December 3, 2020 video advertisement) (emphasis added).

- Using a Nano Wallet, you can "[b]e the only one in charge of your money." www.youtube.com/watch?v=0Rg2-aBYaEE (December 3, 2020 video advertisement).

- "Using a hardware wallet allows you to ***keep your keys completely offline*** even when signing transactions, and is by far the most secure way of managing private keys." http://tinyurl.com/54zm2ydk (statement on Ledger's website originally published on December 18, 2020) (emphasis added).

- "Ledger exists to make you completely autonomous – ***the Nano gives you absolute control over your private keys*** (and therefore your crypto) at all times, while keeping them secure from online threats." http://tinyurl.com/487596va (statement on Ledger's website originally published on December 21, 2020) (emphasis added).

- "The entire point of Ledger's hardware wallet is to offer the best possible security for [private] keys, by keeping them offline. Always." https://tinyurl.com/yc7xkh7t (statement on Ledger's website originally published on January 14, 2021).

- "Whereas hot wallets generate your private keys online, and also store them within a system that is always connected, the Ledger Nano generates your private keys within the device itself, and stores them there too. This means ***your keys will never – ever – be exposed to online threats*** such as hacks and malware, ***and you also don't need to entrust them to another entity***." https://tinyurl.com/yc7xkh7t (statement on Ledger's website originally published on January 14, 2021) (emphasis added).

- "Nano hardware wallets . . . are designed so that ***your private keys never leave the security of the hardware***, even when connecting your wallet to your smartphone or desktop." http://tinyurl.com/mvmxs8bv (statement on Ledger's website originally published on January 14, 2021) (emphasis added).

- A Nano Wallet "gives you ***full ownership*** over your crypto." https://tinyurl.com/esthw9b5 (statement on Ledger's website originally published on January 14, 2021) (emphasis added).

- "With Ledger, we can help make sure your money is, well, yours. Our cold wallets can assist you in taking the plunge so self-custody isn't so scary." http://tinyurl.com/bdh6jenx (statement on Ledger's website originally published on October 1, 2021).

- "The whole premise of a hardware wallet like a Ledger device is to keep both your

> private keys and your recovery phrase offline and away from cyber threats." http://tinyurl.com/bddsud85 (statement on Ledger's website originally published on May 10, 2022).

50. During its advertising campaign, Ledger did not tell consumers it is possible for Ledger to alter the firmware in Nano Wallets such that Ledger or other parties can extract keys from those wallets. In fact, Ledger told consumers the opposite. For example, on November 15, 2022, a Twitter user asked Ledger the following regarding Nano Wallets: "How can you prove to us the customers that the private keys on the device are not leak-able via a firmware update in case someone at the company wants this?" http://tinyurl.com/22wf3xtt (last visited January 4, 2024). Ledger responded: "Hi – your private keys never leave the Secure Element chip [within the Nano Wallet], which has never been hacked. The Secure Element is 3rd party certified, and is the same technology as used in passports and credit cards. A firmware update *cannot extract the private keys from the Secure Element*." http://tinyurl.com/ytsts7xs (last visited January 4, 2024) (emphasis added).

51. Ledger's representations about the security features of its hardware wallets—in particular, the features of its Secure Element chips—helped Ledger differentiate itself from its competitors. Ledger told consumers that "Ledger is the **only** hardware wallet that uses these types of chips." Kirsty Moreland, *The Secure Element and Hardware Wallets: Explained*, LEDGER (February 13, 2020), http://tinyurl.com/4heaar46 (emphasis in original). Ledger also said that "Ledger devices differ from other hardware wallets on the market" because they use Secure Element chips, which provide "industry-leading security" and "the highest level of security for a chip." Kirsty Moreland, *The Secure Element Chip: How It Keeps Your Ledger Secure*, LEDGER (October 23, 2019), http://tinyurl.com/3kc5k9c8. All the while, Ledger maintained that an "important part" of how its devices operate is "that your private keys remain inside the Secure Element" and "the secure element lets you use the private key without allowing it to leave the

chip." Kirsty Moreland, *The Secure Element and Hardware Wallets: Explained*, LEDGER (February 13, 2020), http://tinyurl.com/4heaar46.

52. Based on these and similar claims, Ledger enriched itself and gained market share it otherwise would not have gained. The first cryptocurrency hardware wallet was released by Trezor in 2014. Yet, despite a later start, Ledger overcame Trezor and other competitors in the hardware wallet industry. Ledger has sold over 6,000,000 hardware wallets—more than any other company in the world—and is valued at over $1.4 billion.

E. Ledger's statements regarding its hardware wallets' security features were false and misleading.

53. Ledger's representations that private keys cannot, and could never, leave a Nano Wallet were false. The truth, which Ledger omitted from its statements touting the security features of its Nano Wallets, is that (a) it is possible for private keys to leave the security of Nano Wallets' hardware, (b) it is possible for private keys stored on Nano Wallets to be exposed to the internet, and (c) Ledger itself can write firmware updates that permit the company and other entities to extract private keys directly from customers' Nano Wallets.

54. This became clear when Ledger announced the Recover feature on May 16, 2023. The very purpose of Recover is to allow Ledger to extract customers' seed phrases from their devices online via a firmware update, to create backups for those seed phrases. *See* Anna Baydakova, *Is Ledger's New Bitcoin Key Recovery Feature Safe? Experts Have Doubts*, YAHOO FINANCE (May 19, 2023), https://tinyurl.com/ywhvhc9c.

55. Yahoo Finance explained the feature as follows: "Ledger is preparing to launch a new service called Ledger Recover that splits a wallet recovery phrase—basically, a human-readable form of the private key—into three encrypted shards and distributes them to three custodians: Ledger, crypto custody firm Coincover, and code escrow company EscrowTech. If

somebody loses their recovery phrase, two of the three shards can be combined—pending an ID check—to regain access to the locked funds."[7] *Id.*

56. Similarly, Ledger has explained that, pursuant to the Recover feature, "a pre-BIP39 version of your private key is encrypted, duplicated and divided into three fragments, with each fragment secured by a separate company." *Ledger Recover FAQs*, LEDGER (June 23, 2023), http://tinyurl.com/yck36ttp.

57. After announcing the Recover feature, Ledger admitted the following in a now-deleted Twitter post: "Technically speaking it is and always has been possible to write firmware that facilitates key extraction. You have always trusted Ledger not to deploy such firmware whether you knew it or not." https://archive.is/yxCwy (archive of May 17, 2023 Twitter post from Ledger).

F. Ledger's misrepresentations and omissions regarding its hardware wallets' security features were material.

58. The "news of the [Recover] update provoked a storm of criticism from the crypto community." Anna Baydakova, *Is Ledger's New Bitcoin Key Recovery Feature Safe? Experts Have Doubts*, YAHOO FINANCE (May 19, 2023), https://tinyurl.com/ywhvhc9c. Cryptocurrency users on social media, in particular, were "downright incensed." Jacquelyn Melinek, *Turns Out Ledger Can Hold Some of Your Crypto Wallet's Keys, If You Agree to It*, TECHCRUNCH (MAY 18, 2023), http://tinyurl.com/mt7s7355. The many critical posts included, among others, the following:

- "I will return my Ledger wallet due to your false advertisement. You sold me a device which you said the seed could not leave the secure enclave. But ***you lied*** because it is technically possible and now you are exploiting it so you can get extra revenue. ***Can you not see how misleading this is?*** If you don't refund my money I will start a claim with the credit card I paid because ***I was scammed*** (and

[7] A "wallet recovery phrase" is another term for a seed phrase.

I feel like this)." http://tinyurl.com/2t955nvj (emphasis added).

- "***They've blatantly lied about a critical security feature*** of a device that people are using to store millions of dollars. The trust has been broken, and you're a fool if you think there is any way ledger can regain this trust." http://tinyurl.com/2wvsvkvs (emphasis added).

- "I bought ledgers (multiple) as I was led to believe it was impossible for the secure chip to leak the key, intentional or not. But here is Ledger just adding the very functionality that I thought the chip was designed to prevent. ***I've been scammed***." https://tinyurl.com/2s4kw2va (emphasis added).

- "This is not what your customers bought these devices for. Is it really surprising that ***many users feel violated*** by this announcement?" http://tinyurl.com/2t955nvj (emphasis added).

- "A cold wallet is only cold if it has no mechanism of giving out its seed phrase to the connected devices by design. Now this service seems to suggest they have implemented a way to extract the seed phrase, which can be used by hackers or ledger themselves to steal your coins." http://tinyurl.com/y2zztf93.

- "***The premise the seed stayed secure on the chip*** was [Ledger's] entire business model which we now know ***was a lie all along***." https://tinyurl.com/2s4kw2va (emphasis added).

- "NOBODY NOT A SINGLE PERSON ASKED FOR THIS. Totally annihilates the entire purpose of owning a Ledger." https://tinyurl.com/2s4kw2va.

- "The problem is ***they said it wasn't possible and now they are saying it is possible and always was***. Even if you don't opt in the vulnerability exists. The trust is gone. The reality is nothing has changed except ***they misled their users*** and they were always more vulnerable than they thought." https://tinyurl.com/y95bvy5a (emphasis added).

- "I have been using multiple Ledger hardware wallets since 2017, and I have always been a fan of their products. Their assurance regarding the impossibility of extracting private keys from a Ledger device was something I appreciated. However, their recent announcement about releasing firmware that extracts and uploads the private keys from the device to remote servers has made me permanently loose trust in Ledger." http://tinyurl.com/exna3s2p.

- "I never had much funds on exchanges and put everything on my Ledger asap only to find out that even ***Ledger was dishonest***. It is just impossible to trust anyone or anything within the crypto industry because for most part it is a totally messed up shitshow imo." http://tinyurl.com/2wvsvkvs (emphasis added).

- "I don't think i will stay with ledger. I don't feel comfortable with secrets. ***They lied*** allot ***and sold me on misinformation***." http://tinyurl.com/4vf5w5dh (emphasis added).

- "***Liars gonna lie. Bye Ledger.***" https://tinyurl.com/y95bvy5a (emphasis added).

59. Beyond venting their frustration online, many consumers changed their behavior. They abandoned Ledger altogether and fled to alternative hardware wallet producers. As Yahoo Finance reported, "Trezor sales soared 900% week-over-week after Ledger announced . . . Recover, which gives the company access to users' seed phrases." Owen Fernau, *Trezor Sales Spike 900% Even as Exploit of "T" Model is Revealed*, YAHOO FINANCE (May 25, 2023), http://tinyurl.com/y3c4twtt.

60. The consumer outrage surrounding Recover was so intense that Ledger delayed the new feature's implementation by nearly half a year. Jamie Crawley, *Crypto Wallet Maker Ledger Officially Rolls Out 'Recover,' Unleashing Fresh Round of Snark*, COINDESK (October 24, 2023), https://tinyurl.com/35n56y7k.

61. The outrage was justified. Ledger's misrepresentations and omissions concerned critical and material features of its products. Hardware wallets are more difficult to use than software wallets and cryptocurrency exchanges. Instead of simply logging into a website or downloading an application, hardware wallets require consumers to learn how to use a new device with a unique operating system that does not resemble other, common consumer products. Thus, customers who purchase hardware wallets often do so because they are protecting large sums of money and seek enhanced security features to protect that money. When they purchase hardware wallets, consumers do so specifically because the wallets offer self-custody, offline storage, and safety from third-party access for private keys—the very features about which Ledger lied. Consumers reasonably believed Ledger's representations that Nano Wallets offer those features

given that those features are the entire purpose of a hardware wallet.

G. Ledger's misrepresentations and omissions regarding its wallets' security features were willful and intentional.

62. Ledger's misrepresentations and omissions were willful and intentional. Some hardware wallet producers "open source" the software and/or firmware for their devices, meaning knowledgeable consumers can check the code to determine if it permits, or could permit, the company to extract private keys from those devices. *See* https://trezor.io/security (last visited January 4, 2024).

63. But Ledger does not fully open source its software or firmware. Anna Baydakova, *Ledger's PR Struggle Reveals Uncomfortable Trade-Offs for Crypto Storage*, YAHOO FINANCE (MAY 24, 2023), https://tinyurl.com/ydzmadsn. Nor does it make its hardware designs fully public. Instead, Ledger keeps the most critical information regarding Nano Wallets' functionality secret.

64. Thus, since releasing its first Nano Wallets in 2016, Ledger alone has known the full extent of Nano Wallets' capabilities. Since that time, as the inventor and manufacturer of Nano Wallets, Ledger knew the private keys on its devices could leave the security of the devices' hardware, could be exposed to the internet, and could be extracted via firmware updates.

65. The timeline for the development, and eventual release, of the Recover feature is strong evidence of this knowledge. Ledger began planning for, and developing, the Recover feature over a year before the public learned about it in May 2023. During that time, Ledger must have known it is possible to extract private keys from Nano Wallets' hardware over the internet, given that Ledger was working on a feature designed to do precisely that.

66. Concerningly, even as Ledger planned for and designed the Recover feature, it continued to tell consumers that private keys held on Nano Wallets cannot be extracted from the devices or be exposed to the internet including via firmware updates.

H. Ledger injured Plaintiffs and other consumers by causing them to purchase products they otherwise would not have purchased or causing them to purchase products at prices higher than they otherwise would have paid.

67. Ledger's misrepresentations and omissions regarding its Nano Wallets' security features injured Plaintiffs and similarly situated consumers. Plaintiffs and consumers would not have purchased Nano Wallets at all had they known it is possible for private keys to leave the devices' hardware, that it is possible for private keys held on Nano Wallets to be exposed to the internet, or that it is possible for Ledger to write firmware that facilitates key extraction from Nano Wallets.

68. Plaintiffs and consumers were also harmed by Ledger's misrepresentations and omissions because those misrepresentations and omissions allowed Ledger to charge higher prices for Nano Wallets than Ledger otherwise would have been able to charge. This heightened price was charged both to those who saw and relied on Ledger's misrepresentations and omissions and those who did not, given that both the Ledger Nano S and the Ledger Nano X are sold to all consumers at uniform rates.

69. Finally, Plaintiffs and consumers could not reasonably have discovered the true capabilities of Nano Wallets, or the false and misleading nature of Ledger's statements regarding those wallets, because Ledger did not fully open-source the software and firmware for its devices.

I. Ledger also injured Ledger Nano X purchasers by pushing a firmware update with Recover functionality into their devices.

70. Although Ledger initially delayed the Recover feature, it implemented a firmware update with that feature for Ledger Nano X devices on October 19, 2023, and it says the feature will be coming to the Ledger Nano S Plus soon. Jamie Crawley, *Crypto Wallet Maker Ledger Officially Rolls Out 'Recover,' Unleashing Fresh Round of Snark*, COINDESK (October 24, 2023), https://tinyurl.com/35n56y7k.

71. Subscribing to the Recover feature is currently optional. But Ledger Nano X users *must* implement the firmware update with the Recover *capabilities*. This is because, absent firmware updates, Nano Wallets eventually become unusable. Firmware updates enable continued functionality between Nano Wallets and the applications to which they connect in order to, among other things, facilitate financial transactions. And firmware updates also include vital security updates. For instance, firmware updates include fixes for bugs associated with new versions of computers' and smartphones' operating systems.

72. As a result, Ledger has forced Ledger Nano X users into an impossible choice. They may either let their devices become unusable, or they may accept an update that specifically alters their devices such that they permit private key extraction.

73. The latter is as harmful as the former. As one cryptocurrency entrepreneur pointed out about Recover: "The code path to send private key material over the internet will be on your device, whether you opt in [by subscribing to Recover] or not. Hackers can take advantage of this, and software bugs [are] more likely to leak. Ledger's business trajectory is one of wanton disregard for customer safety. Switch wallets." Okoya David, *"There's No Backdoor": Ledger Responds to Uproar Over Wallet Recovery Service*, DAILYCOIN (May 16, 2023), http://tinyurl.com/ms75dkrd. Ledger's firmware update has injured Ledger Nano X owners, including Plaintiffs who own Ledger Nano X wallets, by reducing the value and usability of the devices they own.

74. Ledger caused this damage intentionally. According to Ledger's CEO, "many people find managing their [seed phrases] daunting or too complex," and Ledger Recover "is designed for *those* people to make secure self custody easier." Rachel Wolfson, *Ledger CEO Says Crypto Key Recovery Service Makes Self-Custody Easier*, COINTELEGRAPH (May 29, 2023),

http://tinyurl.com/mtbevrah (emphasis added). Thus, "the goal behind Ledger Recover is to onboard the *next* 100 million users to the crypto sector." *Id.* (emphasis added). In other words: Ledger made a calculated decision to abandon its existing users, who already paid for devices and who highly value security, to onboard new users, who will pay for new devices and who value convenience over security.

V. CLASS ACTION ALLEGATIONS

75. Plaintiffs bring this action on behalf of a class (the "Illinois Class") defined as follows: "All individuals who, while in the State of Illinois, purchased a Nano Wallet at any time between June 20, 2016 and May 16, 2023."

76. Plaintiffs Edwin Cabrera, Austin Richard, and Mark Sullivan (the "Nano X Plaintiffs") bring this action on behalf of a class (the "Nationwide Nano X Class") defined as follows: "All individuals who, while in the United States of America, purchased a Ledger Nano X at any time between May 15, 2019 and May 16, 2023."

77. The Illinois and Nationwide Nano X Classes are referred to collectively hereafter as the "Classes."

78. The Classes meet the certification prerequisites of Federal Rule of Civil Procedure 23(a) because: (a) the Classes are too numerous for practicable joinder; (b) there are questions of law and fact common to the Classes; (c) Plaintiffs' claims are typical of the Classes; and (d) Plaintiffs and their counsel are adequate representatives of the Classes.

79. The Classes also meet the certification requirements of Federal Rule of Civil Procedure 23(b)(3). Questions of law and fact common to Class members predominate over any questions affecting only individual members, and a class action is superior to other available methods for fairly and efficiently adjudicating this controversy.

VI. CAUSES OF ACTION

80. Plaintiffs seek the following relief based on the following causes of action.

First Cause of Action
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
(Brought by Plaintiffs on Behalf of the Illinois Class)

81. Plaintiffs incorporate by reference and reallege here all foregoing paragraphs of this Complaint.

82. The Illinois Consumer Fraud and Deceptive Business Practices Act ("Consumer Fraud Act") declares unlawful "the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact." 815 ILCS § 505/2. It also makes it unlawful to "represent[] that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have." 815 ILCS § 505/2; 815 ILCS § 510/2(a)(5).

83. Defendants violated these provisions by representing that Nano Wallets have characteristics and benefits that they do not have. Namely, Defendants represented that it is not possible for private keys to leave a Nano Wallet; it is not possible for private keys held on a Nano Wallet to be exposed to the internet; no one aside from a Nano Wallet's owner can access private keys stored on a Nano Wallet; Nano Wallets provide full, complete, and exclusive ownership over private keys; and Defendants themselves could not access private keys held on Nano Wallets regardless of future firmware updates.

84. Defendants also misrepresented the characteristics and benefits of Nano Wallets by omitting material information about those wallets. When Defendants touted the security features of Nano Wallets, Defendants omitted that they could, at any time, access private keys held on Nano Wallets, in particular by implementing firmware updates that extract keys from wallets.

85. Defendants intended for consumers, such as the Illinois Plaintiffs and members of the Illinois Class, to rely on their misrepresentations and omissions so that they would purchase Nano Wallets.

86. Defendants' misrepresentations and omissions caused damage to the Illinois Plaintiffs and the Illinois Class. The Illinois Plaintiffs and the Illinois Class relied on Defendants' representations when purchasing their Nano Wallets, and they would not have purchased their Nano Wallets had they known those representations were false, misleading, or incomplete.

87. Further, Defendants' misrepresentations and omissions permitted them to sell Nano Wallets at prices higher than they otherwise would have been able to sell them. This heightened price was charged both to those who saw and relied on Defendants' misrepresentations and omissions and those who did not. Thus, the Illinois Plaintiffs and the Illinois Class suffered injury in the form of a price premium.

88. As a result, the Illinois Plaintiffs and the Illinois Class each seek and are entitled to: (a) actual damages; (b) punitive damages; (c) injunctive relief; (d) reasonable costs and attorney's fees; and (e) any other relief the Court deems proper. 815 ILCS § 505/10a.

Second Cause of Action
Unjust Enrichment
(Brought by Plaintiffs on Behalf of the Illinois Class)

89. Plaintiffs incorporate by reference and reallege here all foregoing paragraphs of this Complaint.

90. Defendants have been unjustly enriched by their misrepresentations and omissions regarding Nano Wallets. They have sold more hardware wallets (over 6,000,000) than they would have sold absent those misrepresentations and omissions. And they have sold those wallets at higher prices than they could have charged absent their misrepresentations and omissions.

91. Defendants' enrichment has been to Plaintiffs' and the Illinois Class's detriment. Plaintiffs and members of the Illinois Class would not have purchased Nano Wallets at all but for Defendants' misrepresentations and omissions. Certainly, Plaintiffs and members of the Illinois Class would not have paid prices as high but for Defendants' misrepresentations and omissions.

92. There is no justification for Defendants' misrepresentations and omissions or for Defendants' resulting enrichment. Defendants' misrepresentations and omissions were knowingly deceptive.

93. It would violate fundamental principles of justice, equity, and good conscience to permit Defendants to retain the benefits of their misrepresentations and omissions at the expense of Plaintiffs and members of the Illinois Class.

94. As a result, Plaintiffs and the Illinois Class each seek and are entitled to restitution, disgorgement, injunctive relief, and any other relief the Court deems proper.

Third Cause of Action
Violation of the Computer Fraud and Abuse Act
(Brought by the Nano X Plaintiffs on Behalf of the Nationwide Nano X Class)

95. Plaintiffs incorporate by reference and reallege here all foregoing paragraphs of this Complaint.

96. Any entity that "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer" violates the Computer Fraud and Abuse Act ("CFAA"). 18 U.S.C. § 1030(a)(5)(A).

97. Any "person who suffers damage or loss by reason of [such] a violation . . . may maintain a civil action against the violator" if the conduct involves "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" or "a threat to public health or

safety." 18 U.S.C. §§ 1030(g), (c)(4)(A)(i)(I), (c)(4)(A)(i)(IV).

98. Ledger Nano X devices are "protected computers" under the CFAA because (a) they are electronic data processing devices that perform logical, arithmetic, or storage functions in storing and facilitating transactions with private keys, and (b) they are used in and affect interstate and foreign commerce and communication, in that they are used to facilitate interstate and foreign cryptocurrency financial transactions. 18 USC § 1030(e). Ledger Nano X devices are also used in interstate and foreign commerce and communication because they connect to the internet, and to worldwide applications, like the Ledger Live application, through which Ledger Nano X users buy and sell cryptocurrency, and through which they also send and receive messages from other users across the country and the world. *See* Linda Orenes-Lerma, *Discovering Ledger Live Apps and What They Do*, LEDGER (March 31, 2023), http://tinyurl.com/mvd3hv7z.

99. Defendants knowingly caused the transmission of a program, information, code, or command by implementing the firmware update with the Recover functionality for Ledger Nano X devices in October 2023.

100. Through Defendants implementation of the Recover firmware update, Defendants intentionally caused damage without authorization to the hardware wallets owned by the Nano X Plaintiffs and the Nationwide Nano X Class. The Nano X Plaintiffs and the Nationwide Nano X Class did not want or authorize the Recover firmware update, which reduced the value and usability of their devices. Defendants knew implementing the update would damage those devices, yet they pushed the update anyway in an attempt to acquire new customers who value convenience over security.

101. Defendants' implementation of the Recover firmware update has caused loss to one or more persons during a one-year period aggregating at least $5,000 in value. Members of the

Nationwide Nano X Class have spent, in aggregate, over $5,000 replacing their Ledger Nano X devices with alternative devices.

102. Defendants' implementation of the Recover firmware update also threatens public health and safety by placing Defendants' customers at risk of serious financial loss.

103. As a result, the Nano X Plaintiffs and the Nationwide Nano X Class each seek and are entitled to: (a) compensatory damages; (b) injunctive and equitable relief; and (c) any other relief the Court deems proper. 18 U.S.C. §§ 1030(g), (c)(4)(A)(i)(I), (c)(4)(A)(i)(IV).

PRAYER FOR RELIEF AND DEMAND FOR JURY TRIAL

WHEREFORE, Plaintiffs, individually and on behalf of all similarly situated persons, demand a jury trial for all claims so triable and respectfully request that the Court grant the following relief:

A. Certification of this case as a class action pursuant to Federal Rule of Civil Procedure 23;

B. Designation of Plaintiffs as class representatives of the Illinois Class; designation of the Nano X Plaintiffs as class representatives of the Nationwide Nano X Class; and designation of counsel of record as Class Counsel for each of the above-named classes;

C. A declaratory judgment that the practices complained of herein are unlawful under the Illinois Consumer Fraud and Deceptive Business Practices Act and the Computer Fraud and Abuse Act;

D. An award of actual damages, punitive damages, restitution, and other relief provided for under the foregoing causes of action as set forth above;

E. Appropriate equitable and injunctive relief remedying Defendants' misconduct;

F. An award of attorney's fees and costs incurred in this action, including expert fees;

G. Pre-judgment and post-judgment interest, as provided by law;

H. Reasonable service awards for each named Plaintiff; and

I. All other legal and equitable relief that this Court deems necessary, just, and proper.

Dated: January 8, 2024

Respectfully submitted,

/s/ John J. Frawley
One of Plaintiffs' Attorneys

Douglas M. Werman
John J. Frawley
WERMAN SALAS P.C.
dwerman@flsalaw.com
jfrawley@flsalaw.com
77 W. Washington St., Suite 1402
Chicago, Illinois 60602
Phone No.: (312) 419-1008

Attorneys for Plaintiffs and the Putative Classes